JOURNAL OF COMBINATORIAL THEORY, Series A 62, 225–233 (1993)

A Design and a Code Invariant under the Simple Group Co_3

WILLEM H. HAEMERS

Department of Economics, Tilburg University, P.O. Box 90153, 5000 LE Tilburg, The Netherlands,

CHRISTOPHER PARKER*

Department of Mathematics, University of Wisconsin-Parkside, Box 2000, Kenosha, Wisconsin 53141-2000

VERA PLESS

Department of Mathematics, University of Illinois at Chicago, Box 4348, Chicago, Illinois 60680

AND

VLADIMIR D. TONCHEV*

Department of Mathematical Sciences, Michigan Technological University, Houghton, Michigan 49931-1295

Communicated by the Managing Editors

Received October 23, 1990

IN MEMORY OF PROFESSOR MARSHALL HALL

A self-orthogonal doubly-even (276, 23) code invariant under Conway's simple group Co_3 is constructed. The minimum weight codewords form a 2-(276, 100, 1458) doubly transitive block-primitive design with block stabilizer isomorphic to the Higman–Sims simple group *HS*. More generally, the codewords of any given weight are single orbits stabilized by maximal subgroups of Co_3. The restriction of the code on the complement of a minimum weight codeword is the (176, 22) code discovered by Calderbank and Wales as a code invariant under *HS*.

* Part of this work was done while these two authors were at the University of Giessen, Germany, the first as a NATO Research Fellow and the second as a Research Fellow of the Alexander von Humboldt Foundation.

0097-3165/93 $5.00

1. The Design

We assume that the reader is familiar with the basic notions and elementary facts from design and coding theory. Our notation follows that from [1, 3, 7, 12, 13, 15] and for groups [5]. We also use some ideas from the theory of strongly regular graphs and regular two-graphs [3, 6, 14].

The design we are going to discuss can be constructed in the spirit of the work by Hall, Lane, and Wales [8], namely, by using orbits under finite permutation groups.

The Conway simple group Co_3 can be characterized as the full automorphism group acting 2-transitively on a unique regular two-graph Ω on 276 vertices [4, 6, 14]. The group $McL{:}2$, where McL denotes the simple group of McLaughlin [11], is the stabilizer of a point of Ω and acts as a rank 3 group on the remaining 275 vertices. The Higman–Sims simple group HS [9] is a maximal subgroup of Co_3 splitting the vertices of Ω into two orbits of length 100 and 176, respectively, and acting 2-transitively on the orbit of length 176 and as a rank 3 group on the orbit of length 100. The orbit of the set of 100 vertices of G fixed by HS under Co_3 is a 2-design D with 11, 178 blocks, i.e., a 2-$(276, 100, 2 \cdot 3^6)$ design on which Co_3 acts doubly transitively on points and primitively on blocks.

An explicit construction of the design D is obtained by the following permutation presentation of Co_3, which was found by computer using the group theory language CAYLEY. The following two permutations generate Co_3 acting 2-transitively on 276 points:

$$
\begin{aligned}
\alpha = {} & (2\ 24\ 3)(4\ 5\ 7)(8\ 189\ 150)(9\ 184\ 144)(10\ 190\ 149) \\
& (11\ 183\ 143)(12\ 192\ 156)(13\ 191\ 153)(14\ 181\ 154) \\
& (15\ 182\ 155)(16\ 196\ 146)(17\ 194\ 148)(18\ 195\ 147) \\
& (19\ 193\ 145)(20\ 188\ 151)(21\ 186\ 152)(22\ 185\ 141) \\
& (23\ 187\ 142)(25\ 26\ 27)(29\ 49\ 200)(30\ 50\ 199) \\
& (31\ 51\ 198)(32\ 52\ 197)(33\ 57\ 226)(34\ 58\ 225) \\
& (35\ 59\ 228)(36\ 60\ 227)(37\ 55\ 204)(38\ 56\ 203) \\
& (39\ 53\ 202)(40\ 54\ 201)(41\ 47\ 206)(42\ 48\ 205) \\
& (43\ 45\ 208)(44\ 46\ 207)(61\ 121\ 172)(62\ 122\ 171) \\
& (63\ 123\ 169)(64\ 124\ 170)(65\ 127\ 158)(66\ 128\ 157) \\
& (67\ 125\ 160)(68\ 126\ 159)(69\ 138\ 162)(70\ 137\ 161) \\
& (71\ 139\ 164)(72\ 140\ 163)(73\ 118\ 174)(74\ 117\ 173) \\
& (75\ 120\ 176)(76\ 119\ 175)(77\ 131\ 177)(78\ 132\ 178) \\
& (79\ 130\ 180)(80\ 129\ 179)(81\ 134\ 168)(82\ 133\ 167) \\
& (83\ 136\ 166)(84\ 135\ 165)(85\ 91\ 97)(86\ 90\ 98) \\
& (89\ 100\ 95)(92\ 99\ 96)(101\ 107\ 113)(102\ 108\ 114) \\
& (103\ 105\ 115)(104\ 106\ 116)(209\ 232\ 266)(210\ 236\ 268) \\
& (211\ 239\ 272)(212\ 233\ 263)(213\ 231\ 271)(214\ 241\ 265)
\end{aligned}
$$

(215 244 275)(216 237 267)(217 242 269)(218 235 274)
(219 229 264)(220 234 273)(221 240 261)(222 243 262)
(223 230 270)(224 238 276)(245 255 248)(246 258 253)
(247 250 257)(251 252 259);

$\beta =$ (1 117 120 125)(2 78 113 111)(4 167 166 89)
(5 148 174 170)(6 12 56 214)(7 33 250 141)
(8 181 25 71)(9 136 124 119)(10 20 132 178)
(11 31 155 213)(13 35 187 264)(14 193 51 210)
(15 240 191 216)(16 152 59 212)(17 137 60 29)
(18 134 46 55)((19 231 233 61)(21 130 58 232)
(22 199 189 222)(23 118 197 201)(24 86 92 159)
(26 112 70 267)(27 263 235 194)(28 198 62 228)
(30 224 266 218)(32 140 50 154)(34 40 47 248)
(36 244 225 239)(37 153)(38 176 249 87)
(39 165 158 252)(41 150 145 234)(42 256 162 99)
(43 49 52 220)(44 259 192 67)(45 114 79 84)
(48 175 149 247)(53 223 202 207)(54 205 126 122)
(57 188 274 138)(63 80 275 237)(64 72 206 219)
(65 236)(66 186 106 268)(68 271 257 177)
(69 273 171 217)(73 164 246 229)(74 102 103 93)
(76 183 258 243)(77 226 196 242)(81 251 168 115)
(83 109)(84 157 173 97)(88 238)(90 262 245 180)
(91 95 104 108)(94 253 116 98)(96 161 107 269)
(110 270 215 241)(121 143 146 142)(128 221)
(131 190 139 151)(133 211)(135 200)(147 179 265 261)
(163 260)(169 276 272 185)(172 254)
(182 184 208 227)(195 255).

As a base block of our design D we can take the first 100 points 1, 2, ..., 100 since the set-wise stabilizer of this 100-subset turns out to be precisely a group isomorphic to HS.

Since Co_3 has rank 5 permutation representation on the blocks of D, there are at most four (in fact precisely four) intersection numbers: 34, 36, 44, 50. In Table I we give the numbers n_i of blocks intersecting a given

TABLE I

Block Intersection Numbers of D

i	n_i	a_i
34	5600	2608200
36	4125	1536975
44	1100	37950
50	352	11178

block in precisely i points and the number a_i of different intersections of size i ($i = 34, 36, 44, 50$).

Let X denote the set of 276 points of D and let B be a block of D. Since the stabilizer of B, a HS, acts 2-transitively on $X \setminus B$, the blocks intersecting B in a constant number i of points form a 2-design on $X \setminus B$ with 176 points and n_i blocks. The values of n_i for $i = 34, 36, 44$ from Table I correspond to indices of maximal subgroups of HS (cf. [5]). Therefore, the designs obtained in this way are block primitive under HS. In the case $i = 50$, the 352 blocks intersecting B in 50 points split into two classes of 176 blocks each in such a way that if B_1 and B_2 intersect B in 50 points and are disjoint on B, then B_1 and B_2 coincide on $X \setminus B$. Therefore, the restrictions of the blocks intersecting B in 50 points on $X \setminus B$ form the well-known symmetric 2-(176, 50, 14) design discovered first by G. Higman [10].

2. The Code

Since the block size is $100 \equiv 0 \pmod 4$ and all block intersection numbers are even (i.e., the design D is self-orthogonal in the terminology of [16]), the rows of the block-point incidence matrix of D generate a self-orthogonal binary code C_{276} of length 276 with all weights divisible by 4, i.e., C_{276} is a doubly even code. Consequently, the dimension of C_{276} is at most $276/2 = 138$. However, the actual dimension turns out to be as small as 23. A generator matrix for the code is obtained by taking the images of the vector of length 276 and weight 100 with the first 100 positions equal to 1 under the cyclic group of order 23 generated by the following element y of Co_3:

$y = (1\ 191\ 184\ 195\ 28\ 63\ 50\ 245\ 5\ 100\ 11\ 97\ 33\ 135$
$218\ 58\ 84\ 76\ 43\ 181\ 130\ 151\ 231)(2\ 196\ 246\ 222$
$40\ 36\ 203\ 41\ 83\ 68\ 177\ 260\ 47\ 129\ 263\ 34\ 77\ 228$
$85\ 10\ 79\ 150\ 13)(3\ 22\ 271\ 70\ 143\ 145\ 19\ 193\ 138$
$82\ 257\ 221\ 148\ 20\ 4\ 9\ 241\ 103\ 205\ 105\ 242\ 157\ 37)$
$(6\ 175\ 171\ 206\ 252\ 87\ 266\ 140\ 39\ 88\ 155\ 119\ 229$
$185\ 66\ 94\ 136\ 227\ 247\ 152\ 115\ 256\ 7)(8\ 51\ 240$
$108\ 134\ 170\ 192\ 81\ 158\ 189\ 52\ 176\ 141\ 264\ 249\ 212$
$200\ 235\ 166\ 29\ 111\ 96\ 12)(14\ 60\ 210\ 262\ 179\ 118$
$174\ 30\ 42\ 75\ 232\ 54\ 99\ 64\ 202\ 214\ 217\ 46\ 122$
$215\ 188\ 194\ 234)(15\ 244\ 107\ 38\ 71\ 104\ 123\ 163\ 137$
$258\ 144\ 219\ 182\ 153\ 49\ 265\ 261\ 259\ 16\ 272\ 55\ 156$
$35)(17\ 243\ 173\ 61\ 268\ 147\ 48\ 238\ 159\ 124\ 91\ 213$
$236\ 113\ 102\ 109\ 169\ 274\ 216\ 207\ 201\ 31\ 237)(18\ 95$
$160\ 65\ 270\ 230\ 116\ 142\ 44\ 225\ 255\ 226\ 56\ 110\ 89$

233 167 23 276 199 187 198 132)(21 121 93 57 25
275 172 220 139 114 209 73 223 248 90 128 146 204
178 133 208 127 127 74)(24 101 269 53 98 251 186
273 164 92 27 80 131 62 67 86 72 211 190 168 125
45 161)(26 162 197 149 254 32 78 180 165 117 267
112 239 183 224 106 59 126 120 250 154 69 253).

The weight distribution of this code was computed by Jesse Nemoyer and is listed in Table II.

Notes. (i) It is remarkable that the same numbers occur in the last columns of Tables I and II. This implies that for every codeword x, x or $x+\mathbf{1}$ ($\mathbf{1}$ denotes the all-one vector) is the sum of the characteristic vectors of at most two blocks of the D. Furthermore, the minimum weight codewords are precisely the blocks of the design D.

(ii) By the 2-transitivity of Co_3 on the code coordinates, the codewords of any fixed weight w form a 2-design D_w. As seen from the list of maximal subgroups of Co_3 [5] the values A_w (i.e., the number of blocks of D_w) are the indices of maximal subgroups of Co_3:

$$w = 100\colon HS;$$

$$w = 112\colon U_4(3)\colon (2^2)_{133};$$

$$w = 128\colon 2^4 \cdot A_8;$$

$$w = 132\colon 2 \times M_{12}.$$

Since Co_3 has rank 5 on the blocks of $D = D_{100}$ and since D has only 4 non-trivial intersection numbers, Co_3 acts transitively on the pairs of blocks of D with a fixed intersection number. So, by remark (i) Co_3 is transitive on the blocks of D_w for every weight w. This implies that the stabilizer of any (non-zero) codeword is the corresponding maximal subgroup in the list above (there are no other subgroups of the same index). Thus the action of Co_3 on the blocks of D_w is primitive.

TABLE II

The Weight Distribution of the Code C_{276}

i	$A_i = A_{276-i}$
0	1
100	11178
112	37950
128	1536975
132	2608200

(iii) Removing a codeword x of weight 100 and deleting the 100 code coordinates corresponding to the support of x leads to a (176, 22) code C_{176} invariant under the Higman–Sims simple group with weight distribution listed in Table III. In fact, this is precisely the code discovered by Calderbank and Wales [2]. This gives a natural embedding of the Higman–Sims group into the Conway group Co_3. The stabilizers of codewords of weight 50, 56, 64, 66, and 72 are maximal subgroups of HS. The codewords in C_{176} of the first four weights are precisely the restrictions of the blocks of D on $x+\mathbf{1}$ (cf. Table I).

5. A Construction from the McLaughlin Graph

In this section we give a computer-free argument for the 2-rank (i.e., the rank over $GF(2)$) of the incidence matrix of the design D, i.e., the dimension of the code C_{276}, as well as a construction of D and C_{276} based on the McLaughlin graph.

The McLaughlin graph (for short McL) is defined by the rank 3 permutation representation on 275 points of $McL{:}2$ (This defines the graph up to taking complements; we take the one with the smaller degree). McL is a strongly regular graph with parameters (in the notation of [3]) $n=275$, $a=112$, $c=30$, $d=56$, and eigenvalues 112, 2, and -28 with multiplicities 1, 252, and 22, respectively. In fact, McL is the only strongly regular graph with these parameters, but we shall not need this result.

TABLE III

The Weight Distribution of the Code C_{176}

i	$A_i=A_{176-i}$
0	1
50	176
56	1100
64	4125
66	5600
70	17600
72	15400
78	193600
80	604450
82	462000
86	369600
88	847000

We do need, however, some concepts and results from the theory of two-graphs, which we shall briefly explain (see [6, 14]). Let

$$A=\begin{pmatrix} A_1 & A_{12} \\ A_{12}^{\mathrm{T}} & A_2 \end{pmatrix}$$

be the (0, 1)-adjacency matrix of a graph Γ. *Switching* Γ with respect to the set of vertices corresponding to A_1 (or A_2) is the operation that replaces A_{12} by the complement and leaves A_1 and A_2 unchanged. So we obtain a graph Γ' with adjacency matrix (J denotes the all-one matrix):

$$A'=\begin{pmatrix} A_1 & J-A_{12} \\ J-A_{12}^{\mathrm{T}} & A_2 \end{pmatrix}.$$

The graphs Γ and Γ' are called *switching equivalent*. It is indeed easily seen that switching defines an equivalence relation. An equivalence class is called a two-graph. Note that if we switch with respect to the neighbours of a given vertex ∞ of Γ, ∞ becomes an isolated vertex in Γ'. The switching class of McL extended by an isolated vertex ∞ is a two-graph Ω on 276 vertices for which Co_3 is the full automorphism group. Moreover, Co_3 acts 2-transitively on Ω (this implies that Ω is a so-called regular two-graph). From this (we only need 1-transitivity) it follows that, if we isolate any vertex ∞ of a graph in Ω by switching with respect to the neighbours of ∞, the remaining vertices form McL.

THEOREM. *Let A be the (0, 1)-adjacency matrix of the McLaughlin graph. Then the binary code C generated by the columns of the following matrix G,*

$$G=\begin{pmatrix} 1 & 0 & \cdots & 0 \\ \vdots & & A & \\ 1 & & & \end{pmatrix}$$

has dimension 23 and is equivalent to C_{276}.

Proof. Put $E=5A-10I-2J$. Then E has an eigenvalue 0 with multiplicity 253, so rank $E=22$. Therefore 2-rank $E\leqslant 22$, hence 2-rank $A\leqslant 22$. By Lemma 3.4 of [6], Ω has in its switching class a graph which contains $11K_3$ (i.e., 11 mutually disjoint triangles), such that a vertex ∞ outside $11K_3$ is adjacent to precisely one vertex of each triangle. Isolate ∞ by switching with respect to the neighbours of ∞. We see that McL thus obtained has $11K_2$ as an induced subgraph. This implies 2-rank $A\geqslant 22$. So we have 2-rank $A=22$ and hence dim $C=23$.

Next we shall show that Co_3 is an automorphism group of C. By construction, the stabilizer of the first coordinate (the point ∞, say) is $McL{:}2$. So it suffices to show that ∞ can be moved to another point ω by an automorphism of C. Define

$$\tilde{A} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \\ & A & \\ 0 & & \end{pmatrix}.$$

Then $\tilde{A}$ is in the switching class of Ω and its columns together with the all-one vector $\mathbf{1}$ generate C. Switch $\tilde{A}$ to $\tilde{A}'$ such that the point ω becomes isolated. Then $\tilde{A}'$ and $\tilde{A}$ represent isomorphic graphs (McL extended with an isolated vertex). By the switching operation we have added $\underline{\omega}$ or $\mathbf{1}+\underline{\omega}$ ($\underline{\omega}$ denotes the column of $\tilde{A}$ corresponding to ω) to each column of $\tilde{A}$. So the columns of $\tilde{A}'$ are in C. Therefore the isomorphism mapping $\tilde{A}$ to $\tilde{A}'$ maps codewords to codewords and hence is an automorphism of C that moves ∞ to ω. Thus Co_3 is an automorphism group of C.

Finally we show that one block of D is in C. To do so we use another graph in the switching class of Ω which illustrates the action of the group HS (see [14]):

$$\bar{A} = \begin{pmatrix} 0 & N_0 \\ N_0^T & B_0 \end{pmatrix} \quad \begin{matrix} \longleftrightarrow \\ 23 \end{matrix} \quad \begin{matrix} \longleftrightarrow \\ 253 \end{matrix}$$

$$= \begin{pmatrix} 0 & \cdots & 0 & 1 & \cdots & 1 & 0 & \cdots & 0 \\ \vdots & 0 & & & N_1 & & & N_2 & \\ 0 & & & & & & & & \\ 1 & & & & & & & & \\ \vdots & N_1^T & & & B_1 & & & B_{12} & \\ 1 & & & & & & & & \\ 0 & & & & & & & & \\ \vdots & N_2^T & & & B_{12}^1 & & & B_2 & \\ 0 & & & & & & & & \end{pmatrix},$$

$$\begin{matrix} \longleftrightarrow \\ 22 \end{matrix} \qquad \begin{matrix} \longleftrightarrow \\ 77 \end{matrix} \qquad \begin{matrix} \longleftrightarrow \\ 176 \end{matrix}$$

where: N_0 is an incidence matrix of the unique quasi-symmetric 4-(23, 7, 1) design; N_1 is its derived and N_2 its residual design; and B_i ($i=0, 1, 2$) is the adjacency matrix of the block graph of N_i. The respective row sums of N_1, N_2, N_1^T, N_2^T, B_1, and B_2 are 21, 56, 6, 7, 16, and 70. Consider the partition into parts of size 100 and 176 induced by B_2. The group that stabilizes this partition is HS and therefore the part of size 100 is a block d of the

design D. Now isolate, by switching, the upper left entry of $\bar{A}$ in order to obtain A. Then

$$A = \begin{pmatrix} 0 & J-N_1 & N_2 \\ J-N_1^T & B_1 & J-B_{12} \\ N_2^T & J-B_{12}^T & B_2 \end{pmatrix}.$$

The row sums of the block matrices of A are given by

$$\begin{pmatrix} 0 & 56 & 56 \\ 16 & 16 & 80 \\ 7 & 35 & 70 \end{pmatrix}$$

Thus the columns in the middle together with $\mathbf{1}$ add up to the characteristic vector $\underline{d}$ of the block d, hence $\underline{d} \in C$. Also every image of $\underline{d}$ under Co_3 is in C and so $D \subset C$ and therefore $C_{276} \subset C$. Hence $C_{276} = C$.

References

1. Th. Beth, D. Jungnickel, and H. Lenz, "Design Theory," B. I. Wissenschaftsverlag, Mannheim, 1985, and Cambridge Univ. Press, Cambridge, 1986.
2. A. R. Calderbank and D. B. Wales, A global code invariant under the Higman–Sims group, *J. Algebra* **75** (1982), 233–260.
3. P. J. Cameron and J. H. van Lint, "Graphs, Codes and Designs," Cambridge Univ. Press, Cambridge 1980.
4. J. H. Conway, Three lectures on exceptional groups, *in* "Finite Simple Groups" (M. B. Powell and G. Higman, Eds.), pp. 215–247, Academic Press, New York, 1971.
5. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, "Atlas of Finite Groups," Clarendon, Oxford, 1985.
6. J. M. Goethals and J. J. Seidel, The regular two-graph on 276 vertices, *Discrete Math.* **12** (1975), 143–158.
7. M. Hall, Jr., "Combinatorial Theory," 2nd ed., Wiley, New York, 1986.
8. M. Hall, Jr., R. Lane, and D. Wales, Designs derived from permutation groups, *J. Combin. Theory* **8** (1970), 12–22.
9. D. G. Higman and C. C. Sims, A simple group of order 44, 353, 000, *Math. Z.* **105** (1968), 110–113.
10. G. Higman, On the simple group of D. G. Higman and C. C. Sims, *Illinois J. Math.* **13** (1969), 74–80.
11. J. McLaughlin, A simple group of order 898, 128, 000, *in* "Theory of Finite Groups" (R. Brauer and C. H. Sah, Eds.), pp. 109–111, Benjamin, New York, 1969.
12. F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, 1977.
13. V. Pless, "Introduction to Coding Theory," Wiley, New York, 1986.
14. D. E. Taylor, Regular 2-graphs, *Proc. London Math. Soc. Ser. 3* **35** (1977), 257–274.
15. V. D. Tonchev, "Combinatorial Configurations," Longman Scientific and Technical, Wiley, New York, 1988.
16. V. D. Tonchev, Self-orthogonal designs, *Contemp. Math.* **111** (1990), 219–235.